UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Device in the Custody of the Alamance County Sheriff's Office Which is Related to the Investigation of Michael Robert Kwasniewski

Case No. 18MJ328

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Device located in Bin ACDC, PR, 1, 161 at the Alamance County Sheriff's Office, more particularly described in Attachment A, attached hereto and made part hereof.

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 912	Impersonating an Officer or Employee of the United States

The application is based on these facts:

See attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Jason N. Morton, Senior Inspector
Printed name and title

Sworn to before me and signed in my presence.

Date: 11/6/18 10:55 AM

Judge's signature

City and state: Durham, North Carolina

Joe L. Webster, United States Magistrate Judge
Printed name and title

1:18MJ328

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Jason Morton, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Deputy United States Marshal with the United States Marshals Service ("USMS"), and have been since May 2008. I am currently assigned as the Sex Offender Investigations Branch Senior Inspector. In this capacity, I am assigned to work investigations involving the Adam Walsh Act, Sex Offender Registry violations, and other violations of federal criminal law throughout the Middle District of North Carolina, including Forsyth County. I have participated in ordinary methods of investigation, including but not limited to, consensual monitoring, physical surveillance, interviews of witnesses and subjects, the use of confidential informants, and pen registers. Through formal and on the job training, I have developed experience in investigations dealing with offenses set forth in the United States Code. As a USMS Senior Inspector, I am authorized to investigate violations of federal law and to execute warrants issued under the authority of the United States.

2. This affidavit is submitted in support of an application for a warrant to seize and search the property specifically described in Attachment A, the cell phone located at the Alamance County Sheriff's Office in Bin ACDC,

PR, 1, 161 (the "DEVICE"), for contraband, evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 912 which items are more specifically described in Attachment B of this Affidavit.

3. The statements in this affidavit are based on my own investigation into this matter as well as on information provided to me by other law enforcement officials and lay witnesses. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that the DEVICE, and the materials contained therein, constitute contraband, evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 912.

4. As noted above, this investigation concerns violations of 18 U.S.C. § 912, which prohibits, inter alia, a person from falsely assuming or pretending to be an officer or employee acting under the authority of the United States or any department, agency, or officer thereof, and acting as such.

5. The following definitions apply to Attachment B and this Affidavit:

a. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data

storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones ("cell phones") and devices. *See* 18 U.S.C. § 1030(e)(1).

b. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

c. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in

electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

d. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

e. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail,

remote storage, and co-location of computers and other communications equipment.

f. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

SUMMARY OF THE INVESTIGATION

6. On September 26, 2018, the USMS for the Middle District of North Carolina received correspondence from the USMS for the Eastern District of North Carolina requesting assistance with an investigation into Michael Robert KWASNIEWSKI, who was suspected of impersonating a Deputy U.S. Marshal in Duplin County, North Carolina. Specifically, during an encounter with law enforcement in Duplin County, KWASNIEWSKI represented himself as a Deputy U.S. Marshal from Greensboro, known as "Kwas," and gave what appeared to be authentic USMS gear to a Duplin County Deputy Sheriff. During the encounter, KWASNIEWSKI was driving a white Chevrolet Suburban. Law enforcement also observed two AR-15 type rifles and tactical gear in the trunk of the Chevrolet Suburban.

7. According to a search of the North Carolina Division of Motor Vehicles, KWASNIEWSKI resides at 1512 Reynard Drive, Kernersville, North Carolina 27284. The following vehicle is registered to KWASNIEWSKI: a 2004 Nissan Titan, bearing license plate number ZXZ3740. To my knowledge, no other vehicles are registered to KWASNIEWSKI in North Carolina.

8. I drove by KWASNIESKI's known home and work addresses to look for the white, Chevrolet Suburban driven by KWASNIESKI during the encounter with the Duplin County Sheriff's Deputy. I did not locate the Suburban, but noted that a silver Ford Mustang with temporary tags was parked in the driveway of the 1512 Reynard Drive, Kernersville, North Carolina 27284.

9. On October 14, 2018, the Winston-Salem Police Department came into contact with KWASNIEWSKI who claimed to be with the USMS. He arrived at the scene in a silver Ford Mustang, bearing license plate number FHB-5803. KWASNIEWSKI was wearing MultiCam camouflage with a U.S. Marshals arm patch, a tactical vest with the words "POLICE U.S. MARSHAL" on the front in big letters, and had what appeared to be a USMS badge draped around his neck. He presented credentials to members of the WSPD, including a document identifying him as Deputy U.S. Marshal, Michael Robert

Kwasniewski. KWASNIEWSKI was visibly armed with a Glock 9mm handgun and additional magazines of ammunition.

10. During his encounter with WSPD, KWASNIEWSKI asked for assistance in locating a subject who had recently moved to the area and had pending charges for assaulting women and children. KWASNIEWSKI used a cell phone to display a photograph of the individual he was attempting to locate.

11. KWASNIEWSKI also offered to give one of the officers a "US MARSHALS" shirt and attempted to locate a shirt in the trunk of the silver Ford Mustang. After being unable to locate the shirt, he told officers he must have forgotten to bring the shirt.

12. KWASNIEWSKI was ultimately arrested by the WSPD and was charged with Impersonating a Law Enforcement Officer in violation of N.C. G.S. 14-277. WSPD seized several items, including: a Glock, Model 17 Gen 4, 9mm semi-automatic pistol with a fully loaded magazine; multiple magazines and other ammunition, including a loaded AR-15 .223 magazine; a duty belt with firearm holster and handcuffs; various clothing and tactical gear bearing the U.S. Marshals title and insignia; and false U.S. Marshals badge,

identification cards, and credentials. The cell phone KWASNIEWSKI used to display the image of the alleged "subject" was not seized by police.

13. During a post-Miranda interview, KWASNIEWSKI provided his address as the 1512 Reynard Drive, Kernersville, North Carolina 27284. KWASNIEWSKI also stated that the Ford Mustang belonged to his roommate, Kathleen Mae Kizer. A search of the North Carolina Division of Motor Vehicles traced the Ford Mustang to Ms. Kizer.

14. On October 23, 2018, I inspected the badges and credentials seized by WSPD. Both badges and credentials initially appeared externally to be legitimate. After closer inspection all items were determined to be fraudulent, but of such remarkable quality that would require more than a cursory inspection to make that determination.

15. I also canvassed local firearms retailers to determine if they were familiar with KWASNIEWSKI. Employees at the ProShots shooting range and gun shop in Winston-Salem were very familiar with him. According to the manager, KWASNIEWSKI was a frequent customer who had purchased "tons of guns" from ProShots and was seen wearing "U.S. Marshal" clothing. To date, the investigation has revealed that KWASNIEWSKI purchased twenty firearms from ProShots from on or about April 2012 to March 2018.

16. I also learned that, on August 19, 2018, KWASNIEWSKI asked a ProShots employee if he could use the range after hours as a law enforcement official and was given permission to do so. Transaction records provided by ProShots confirm that KWASNIEWSKI was charged $60.00 for "RANGE-Private Security/LE Use."

17. On November 2, 2018, the USMS executed an arrest warrant for KWASNIEWSKI at the 1512 Reynard Drive, Kernersville, North Carolina 27284 based on an indictment charging KWASNIEWSKI with Impersonating an Officer or Employee of the United States in violation of Title 18, United States Code, Section 912. While lawfully inside the 1512 Reynard Drive, Kernersville, North Carolina 27284, I saw a USMS hat and badge in plain view as well as a Glock handgun with a tactical light in KWASNIEWSKI's bedroom. I did not seize the described items.

18. Also on November 2, 2018, in a post-*Miranda* interview with USMS, KWASNIEWSKI stated that he had purchased the USMS items on eBay.

19. Following his arrest, law enforcement took custody of KWASNIEWSKI's personal effects, including a cell phone located on his person

(*i.e.*, the DEVICE). These items are currently located in Bin ACDC, PR, 1, 161 at the Alamance County Sherriff's Office.

BACKGROUND ON IMPERSONATION OF LAW ENFORCEMENT, COMPUTERS, AND THE INTERNET

20. Based on my training, experience, and information communicated to me by other law enforcement officers knowledgeable in the area, I know the following about impersonation of law enforcement:

a. Individuals who impersonate law enforcement officials tend to obtain instrumentalities of their crimes, such as fraudulent identification, counterfeit badges, uniforms, and other paraphernalia, via the internet.

b. In modern American culture, most individuals possess multiple devices that have the ability to connect to the internet (*e.g.*, tablets, desktop computers, laptop computers, and mobile phones). Many individuals also keep prior versions of their devices (*e.g.*, prior cell phones and prior computers). This is the case because (1) individuals are often reluctant to discard devices that frequently contain significant personal information and (2) current devices may malfunction and prior versions can often be used until the current device is repaired or replaced.

c. Mobile devices are commonly set to backup automatically when connected to a computer. Individuals have been known to plug their mobile devices into computers causing data to be backed up to the computer without even realizing that this data transfer is occurring. Mobile devices can also be set to sync automatically with Cloud storage and paired devices. For example, an individual using Google Pictures or iCloud Photo Library may have images taken using a mobile device automatically backup to cloud storage and pushed out to, or "synced," with their other computer devices.

d. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, application data, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints"

in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

21. As described in Attachment B, this application seeks permission to seize the DEVICE and search for records that might be contained therein. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of all electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

22. I submit that there is probable cause to believe those records will be stored on the DEVICE, for at least the following reasons:

a. Based on my knowledge, training, and information related to me by knowledgeable law enforcement agents, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer,

the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are

sometimes automatically downloaded into a temporary Internet directory or "cache."

23. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cell phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel

who have specific expertise in the type of computer, software application, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that

a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

CONCLUSION

24. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are contained in Attachment A, the DEVICE. I respectfully request that this Court issue a search warrant for the DEVICE, the property described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

Jason Morton
Senior Inspector
United States Marshals Service

Sworn and subscribed before me this 6th day of November 2018. 10:55 AM

Joe L. Webster
United States Magistrate Judge
Middle District of North Carolina

ATTACHMENT A

ITEM TO BE SEIZED AND SEARCHED

The DEVICE to be seized and searched, relating to the investigation of Michael Robert KWASNIEWSKI, is a cell phone located in Bin ACDC, PR, 1, 161 at the Alamance County Sherriff's Office. The Alamance County Sheriff's Office took custody of the DEVICE following KWASNIEWSKI's arrest on November 2, 2018, based on an indictment charging KWASNIEWSKI with Impersonating an Officer or Employee of the United States in violation of Title 18, United States Code, Section 912.

ATTACHMENT B

ITEMS TO BE SEIZED

The DEVICE referenced in Attachment A and the following materials contained therein, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Section 912:

1. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

g. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

h. records of or information about Internet Protocol addresses used by the COMPUTER;

i. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses revealing an interest in the United States Marshal Service ("USMS") and items used by USMS or that could be used to impersonate a USMS employee.

2. Records and information relating to violations of the statutes described above in the form of:

a. Records and information referencing or revealing interest in the United States Marshal Service ("USMS") or other law enforcement agencies;

b. Records and information referencing or revealing acts or plans to impersonate law enforcement or insinuate that one is a law enforcement officer;

c. Records and information referencing or revealing the purchase or creation of clothing, tactical gear, and items displaying USMS insignia or that could be used to impersonate a law enforcement officer;

d. Records and information referencing or revealing the use of eBay.

3. During the course of the search, photographs of the searched device may be taken to record the condition thereof.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing

logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.